

VZCZCXRO1411
RR RUEHAG RUEHDF RUEHIK RUEHLZ RUEHROV RUEHSR
DE RUEHLI #0071/01 0340735
ZNR UUUUU ZZH
R 030735Z FEB 09
FM AMEMBASSY LISBON
TO RUEHC/SECSTATE WASHDC 7339
INFO RUCNMEM/EU MEMBER STATES
RHMFIUU/FBI WASHINGTON DC
RHEFHLC/HOMELAND SECURITY CENTER WASHINGTON DC
RUEAIIA/CIA WASHDC

UNCLAS SECTION 01 OF 08 LISBON 000071

SIPDIS

S/CT KEN MCKUNE, NCTC, AND DHS

E.O. 12958: N/A

TAGS: [KVPR](#) [PTER](#) [PREL](#) [PGOV](#) [PINR](#) [CVIS](#) [ASEC](#) [KHLS](#) [PO](#)

SUBJECT: PORTUGAL: INFORMATION ON GOVERNMENT PRACTICES -
INFORMATION COLLECTION, SCREENING, AND SHARING

REF: 07SECSTATE 133921

¶1. (U) This message responds to the reftel questions concerning Portugal's information collection, screening, and sharing practices.

¶A. Watchlisting:

-- If host government maintains a "watchlist," how many records does the watchlist contain, and how many are terrorist-related? Which ministry or office maintains the watchlist?

The Ministries of Justice, Interior, and Defense keep such records, however data on number of records and specific types are not made readily available and considered sensitive information not for distribution.

¶B. Traveler Information Collection:

-- What are the country's policies (legislation, mandates, etc.) on collecting information from travelers arriving in the country?

Decree Law 57/2007 from July 4, 2007 updates the border control legislation and three addenda approve information collection models for people entering Portugal, residing in Portugal as refugees, and requesting an extended stay (Portaria 395/2008, 396/2008, and 297/2008 respectively). Portuguese Immigration (Servico de Estrangeiros e Fronteiras - SEF) is responsible for all controls.

-- Are there different policies for air, sea, and land entry and for domestic flights? Since Portugal is a Schengen nation, there is no set border control for land entries. Air and sea entry are treated as the same.

-- Who collects traveler information?

SEF is responsible for collecting and storing traveler information from the airlines, port authorities, travel agencies, and hotels. According to Portuguese Law 57/2007, air transportation authorities are responsible for transmitting their final flight manifest including the name, travel documentation used, date of birth, entry point, and hour of arrival to SEF. Sea transportation companies and fishing vessels that enter Portuguese territory from international waters are also required to submit their manifest to SEF and must notify SEF of stowaways up to 48 hours before arriving and within two hours of departure.

-- What are the policies of the collecting agency to share that information with foreign governments?

SEF may share the information, upon a foreign government request, pursuant to the domestic law on international judiciary cooperation.

-- Does the host government collect Passenger Name Record (PNR) data on incoming commercial flights or vessels? Is this data used for intelligence or law enforcement purposes

to screen travelers? Does host government have any existing treaties to share PNR data?

Yes, the Portuguese government does collect this data for intelligence and law enforcement purposes. Portugal is included in the EU regulations on PNR data.

-- If applicable, have advance passenger information systems (APIS), interactive advanced passenger information systems (IAPIS), or electronic travel authority systems been effective at detecting other national security threats, such as wanted criminals?

Yes, we do not have statistical information on this issue, but believe the systems have been effective in screening passengers.

1C. Border Control and Screening:

-- Does the host government employ software to screen travelers of security interest?

The host government employs software to screen all non-Schengen travelers and the GOP recently requested CODIS software to enhance screening abilities. However, Portugal is a member of the EU's Schengen Agreement, and under its provisions, Portugal, as well as the other Schengen participants, abolished routine immigration controls for persons traveling by air, sea or land between signatory States. Portugal's only land border is with Spain, and border checkpoints between the two countries are normally no longer operational.

-- Are all travelers tracked electronically, or only non-host-country nationals? What is the frequency of travelers being "waived through" because they hold up what

LISBON 00000071 002 OF 008

appears to be an appropriate document, but whose information is not actually recorded electronically? What is the estimated percentage of non-recorded crossings, entries and exits?

All arrivals at airports and seaports are reviewed by SEF, but only foreigners from non-Schengen nations are recorded. At international ports of entry, SEF officers have access to computerized databases that contain information regarding outstanding warrants, criminal convictions, lost and stolen passports, and stolen blank passport data and persons who were previously denied Schengen visas or admission to a Schengen country. Portugal's international airports are monitored by SEF and Customs officials. A minimum check (a quick, straightforward verification of the validity of the document and an examination for signs of falsification or counterfeiting) is the rule for EU citizens and other persons enjoying the Community right of free movement (such as the family members of an EU citizen).

Portuguese airports use an automated passport control system called "RAPID" for EU citizens over 18 years old holding biometric e-passports. RAPID uses facial recognition technology and performs the same checks as a human immigration officer including check a database for stolen, misappropriated, lost and invalidated documents, review the validity of the travel document, and flag the presence of signs of falsification or counterfeiting.

SEF controls entry and exit via Portugal's external borders and its operations follow guidelines from the Community Code on the rules governing the movement of persons across borders (Schengen Borders Code) established by the European Parliament and the EU Council on 15 March 2006. External borders may be crossed only at border crossing-points. Operational cooperation is coordinated by the European Agency for the Management of Operational Cooperation at the External Borders of the Member States (FRONTEX).

We cannot estimate the percentage of non-recorded crossings of the total entries because of the unrecorded land crossings due to the Schengen agreement.

-- Do host government border control officials have the authority to use other criminal data when making decisions on who can enter the country? If so, please describe this

authority (legislation, mandates, etc).

Yes. Under the Schengen Borders Code, the control of movement of persons across borders includes the mandatory check of all national and international criminal and police databases especially the SEF database and the national and Interpol fugitive intelligence database and the entry refusal Schengen Information System, which has information about individuals who are considered to be a threat to public policy, internal security, public health.

-- What are the host government's policies on questioning, detaining and denying entry to individuals presenting themselves at a point of entry into the country? Which agency would question, detain, or deny entry?

Portugal's policy on denying entry is outlined in Article 32 of Portugal's Decree Law 57/2007. In particular, the GOP reserves the right to deny entry to those who do not meet the legal entry requirements, who are on the Schengen "do not admit" list, who are on Portugal's national "do not admit list," are considered a danger or threat to public order, national security, public health, or against diplomatic interests. SEF is the responsible agency for detentions and denied entries.

Pursuant to the provisions of the Portuguese immigration law, Portuguese Immigration (SEF) has the authority to question and deny entry into the country of any non-Portuguese nationals. Additionally, SEF has the authority to detain an individual for the maximum period of 48 hours. Detention will be subject to the scrutiny of a judicial authority within that 48 hour holding period. During the review, the judicial authority hears the reasons for the detention, informs the person detained thereof and questions the detainee to allow him or her to present a defense.

-- How well does information sharing function within the host government, e.g., if there is a determination that someone with a valid host-government visa is later identified with terrorism, how is this communicated and resolved internally? Information sharing seems to work well, however the Judicial Police (FBI equivalent), the intelligence services, and SEF all report to different ministries in the Portuguese government. In 2008, the Portuguese government established a new Secretary General to coordinate the various domestic security efforts.

Additional background information: The Intelligence System of

LISBON 00000071 003 OF 008

the Portuguese Republic (SIRP) coordinates the two separate Portuguese intelligence services. The Security Intelligence Service (SIS) guarantees Portugal's security against sabotage, terrorism, espionage and the practice of acts who, by their nature, could disrupt the rule of law. The Defense Strategic Intelligence Service (SIED) focuses externally to guarantee Portugal's national independence, national interests, and security. Both intelligence services report to the Prime Minister.

1D. Biometric Collection:

-- Are biometric systems integrated for all active POEs? What are the systems and models used?

Yes, international airports in Portugal use an automated passport control system called "RAPID." The system is available only to EU citizens over 18 and holders of biometric e-passports. RAPID uses facial recognition technology and performs the same checks as a human immigration officer, such as data base checks for stolen, misappropriated, lost and invalidated documents, reviewing the validity of the document authorizing the legitimate holder to cross the border, and flagging the presence of signs of falsification or counterfeiting.

RAPID (Automatic Identification of Passengers Holding Traveling Documents) combines the operations of reading and checking electronic passports with an innovating feature for assessing biometric data which operates an automatic gate opening device. This device checks whether the electronic passports is genuine, and validates the data stored on the

chip. It then appraises the passenger's identification by establishing a comparison between the photo stored on the chip and the information of the passenger in loco, automatically opening the border gate when the features of both images are coincident. RAPID was made secure by an intelligent system that allows the entry of a single passenger each time and automatically adjusts the reading camera to his or her height.

-- Are all passengers screened for the biometric or does the host government target a specific population for collection (i.e. host country nationals)? Do the biometric collection systems look for a one to one comparison (ensure the biometric presented matches the one stored on the e-Passport) or one to many comparison (checking the biometric presented against a database of known biometrics)?
All EU citizens with e-passports over eighteen years old are screened. Portugal uses a system of one-to-many comparisons.

-- If biometric systems are in place, does the host government know of any countermeasures that have been used or attempted to defeat biometric checkpoints?
No, it is not aware of any.

-- What are the host government's policies on collecting the fingerprints of travelers coming into the country?
One program exists. Portugal has started in Dakar, Senegal a pilot program conducted on a voluntary basis only, called BIODIV. BIODIV includes the capture of biometrics data (2D face, 10 fingerprints) of a visa applicant at a Portuguese consular post, forwarding the captured data to be stored and searched in a central AFIS, and the verification of the biometrics data of the visa holder at the port of entry. Portugal recently went live based on the complete biometric visa application process in Dakar, Senegal, with participants arriving at Lisbon airport.

-- Which agency is responsible for the host government's fingerprint system?
Portuguese Immigration, SEF

-- Are the fingerprint programs in place NIST, INT-I, EFTS, UK1 or RTID compliant?
The fingerprint program in place is the finger image data interchange format standard: ISO 19794-4 (code WSQ).

-- Are the fingerprints collected as flats or rolled? Which agency collects the fingerprints?
The fingerprints are collected digitally as flats.

1E. Passports:

-- If the host government issues a machine-readable passport containing biometric information, does the host government share the public key required to read the biometric information with any other governments? If so, which governments?
We attempted to contact authorities from the Portuguese Mint in charge of this program, but were unable to confirm at this

LISBON 00000071 004 OF 008

time. It is likely that Portugal shares information with its Schengen partners.

-- Does the host government issue replacement passports for full or limited validity (e.g. the time remaining on the original passports, fixed validity for a replacement, etc.)?
The government issues a new passport for full validity.

-- Does the host government have special regulations/procedures for dealing with "habitual" losers of passports or bearers who have reported their passports stolen multiple times?
Yes. The adjudicators report the situation to the police for possible investigation and, if necessary, judicial action.

-- Are replacement passports of the same or different

appearance and page length as regular passports (do they have something along the lines of our emergency partial duration passports)?

There are no replacement passports. In exceptional circumstances, namely, the adjudicating entity has no authority to issue regular passports (as is the case of Portuguese consular offices overseas) or the electronic passport system is down, a temporary passport may be issued to the applicant. This passport is an eight-page document valid for six months only, and is neither biometric nor machine readable.

-- Do emergency replacement passports contain the same or fewer biometric fields as regular-issue passports?
Emergency passports do not contain biometric information.

-- Where applicable, has Post noticed any increase in the number of replacement or "clean" (i.e. no evidence of prior travel) passports used to apply for U.S. visas?
No, we have not seen any increase.

-- Are replacement passports assigned a characteristic number series or otherwise identified?
No, they do not have any special numbers or identification.

F. Fraud Detection

-- How robust is fraud detection and how actively are instances of fraud involving documents followed up?
Portuguese Immigration (SEF) is responsible for the investigation and detection of fraudulent documents. Fraud detection is taken very seriously and instances involving recent bank fraud cases and large company malfeasance have been aggressively pursued. The fraud detection department and forensic lab conduct highly sensitive investigations. Once an investigation is completed, it is turned over to the courts for prosecution. The Embassy has visited the facilities and finds it both professionally run and capable of handling sensitive investigations.

-- How are potentially fraudulently issued documents taken out of circulation, or made harder to use?
Portugal is one of the better EU nations in making its documents safer and more difficult to forge by way of various up to date security document features (i.e. holographic, light latent imagery, etc.). SEF is also involved in the process of establishing document security features. Whenever fraudulent documents are found, they are confiscated and voided.

G. Privacy and Data Security

-- What are the country's policies on records related to the questioning, detention or removal of individuals encountered at points of entry into the country?
Pursuant to Portuguese immigration law, Portuguese Immigration (SEF) has the authority to question and deny entry into the country of any non-host country nationals. If admission into the country is denied on grounds of fraudulent documents, the document is confiscated and the individual is immediately returned pursuant to the Chicago Convention. If the individual cannot be deported within 48 hours, he or she must appear before a judicial authority for a hearing. SEF will question and interview the individual and where necessary, will call the Judicial Police (PJ) to intervene and interrogate the more serious cases. An illegal entry into Portugal often requires repatriation of the individual by the same airline. These individuals are often held at detention centers at the airport. Aliens removed from Portuguese territory by SEF are banned from returning to the country for a minimum of five years.

-- How are those records stored, and for how long?

LISBON 00000071 005 OF 008

The Portuguese government stores records in the National Integrated Information System. Personal information is kept in a temporary file by SEF for 48 hours unless needed for

legal reasons, as outlined in law 67/1998 governing personal information. Transportation companies must delete the information within 24 hours of transmitting the data to SEF. Personal data entered into the Schengen Information System for the purposes of tracing persons is kept only for the time required to meet the purposes for which they were supplied and/or for legal proceedings. Alerts inserted by any EU Schengen member state must be reviewed after three years of entry of the alert in order to evaluate the need for continuing storage of such data.

-- What are the country's restrictions on the collection or use of sensitive data?

Only cleared law enforcement personnel may access the data. The name and official purpose from the officer are required as well to view any records. Collection or use of sensitive data relating to the movement of persons using information from the European Union's Schengen Information System was established by law in 1994, pursuant to the Schengen Convention. The law created the control and monitoring mechanisms for the Schengen Information System. A central Schengen database facility operates under the direction of Portuguese Immigration Service (SEF) and a designated official at the Ministry of Internal Administration (MAI). The Data Protection National Commission (Comissao Nacional de Proteccao de Dados, or CNPD) is the national control authority entrusted with the supervision of the national part of the Schengen Information System, and with the verification that the processing and use of the data does not violate the rights of the person. The rights to access, alter records, and delete information shall be exercised by a person demonstrating a legitimate, direct and personal interest, as provided in the Schengen Convention, by means of the national control authority.

-- What are the requirements to provide notice to the public on the implementation of new databases of records?

The Portuguese Constitution has extensive provisions on protecting privacy, secrecy of communications and data protection. The law on personal data protection established the conditions applicable to automatic processing, connection, transmission and use of databases and guarantees its protection by means of an administrative body, the National Data Protection Commission (Comissao Nacional de Proteccao de Dados, or CNPD). The Commission is an independent agency that is directly responsible to Parliament. Its must register existing databases with private data, authorize and control such databases, issue directives, and oversee the Schengen Information System (SIS).

Implementation of new databases of records is sent by the executive branch to the Portuguese Parliament for approval. When the new database is authorized, it becomes public through the publication of the law in the Government Official Gazette.

-- Are there any laws relating to security features for government computer systems that hold personally identifying information?

There are varied levels of access to security features and these are normally held in government protected computer systems.

-- What are the rules on an individual's ability to access data that homeland security agencies hold about them?

The Schengen Convention itself recognizes the rights of individuals. These include the right to access information in the Schengen Information System (SIS); the right to correct data where there is a de jure or de facto mistake; the right to apply to the courts or competent authorities to demand that data be corrected, deleted or that damages be awarded; the right to ask that data to be checked and to question the reason for data collection. Since Portugal is a signatory to the Schengen Convention, all requests for access to personal data must follow the provisions of the Schengen Convention's article 109, article 6 of Portuguese Law 2/94, and/or article 11 of Portuguese Law 67/98. Any citizen or alien may request verification on whether there is an alert

in his or her name in the Schengen database. In addition, he/she may request a correction or deletion of personal data, in accordance with article 110 of the Schengen Convention.

-- Are there different rules for raw data (name, date of birth, etc.) versus case files (for example, records about

LISBON 00000071 006 OF 008

enforcement actions)?

No, all records fall within the same database. Cases under investigation or considered highly confidential will be kept in a separate database only with written agreement from the prosecutor's office.

-- Does a non-citizen/resident have the right to sue the government to obtain these types of data?

Yes, in accordance with data protection principles, individuals have specific rights under the Schengen Convention, whether they are nationals of Schengen nations or not. The rights include the right of access to personal data stored in the SIS, the right to a rectification when data are factually inaccurate or unlawfully stored, the right to bring before the courts or competent authorities an action to correct or delete incorrect data or to obtain compensation.

H. Immigration Data Bases:

-- What computerized immigration databases are used to track entries and exits?

The Schengen Information System and national Portuguese databases are used to track entries and exits.

-- Is the immigration database available at all ports of entry (POEs)? If immigration databases are available at some POEs, but not all, how does the host government decide which POEs will receive the tool?

Databases are available at all ports of entry but not at all potential land border crossings.

-- What problems, if any, limit the effectiveness of the systems? For example, limited training, power brownouts, budgetary restraints, corruption, etc.?

No problems.

-- How often are national immigration databases updated?

Databases are updated daily with new information.

I. Watchlist and Information Sharing:

-- Is there a name-based watchlist system used to screen travelers at POEs?

Yes, at border checkpoints and in the general watchlist computer database that only police can access.

-- What domestic sources of information populate the name-based watchlist, i.e. names of deported persons, terrorist lookouts, criminal wants/warrants?

Name and date/place of birth are included. Other identifiers include: parents' names, marital status, home address, national identity card number, social security number, Prior criminal offense records, traffic offense data (to include unpaid tickets, DUIs), non-compliance with court-related summons, wants/warrants and some child predator information at a different access level.

-- What international watchlists does the host government use for screening individuals, e.g. Interpol or TSA No Fly lists, UN, etc.?

INTERPOL, EUROPOL and other international intelligence sources.

-- What bilateral/multilateral watchlist agreements exist between host government and its neighbors?

Agreements exist with all EU nations as well as others with the US, Spain, and Brazil. Agreements with Spain and Brazil are in response to Spanish terrorist group ETA and North African terrorists transiting the area and drug producing/transiting in the case of Brazil.

1J. Biometrics:

-- Are biometric systems in place at ports of entry (air, land, sea)? If no, does host government have plans to install such a system?

Biometric systems are in place for air and sea entries as outlined above.

-- If biometric systems are available at some POEs, but not all, how does the host government decide which POEs will receive the tool?

All but land entries are in use as a result of the Schengen agreement.

-- What biometric technologies, if any, does the host government use, i.e. fingerprint identification, facial recognition, iris recognition, hand geometry, retinal identification, DNA-based identification, keystroke dynamics, gait analysis? Are the systems ICAO compliant?

LISBON 00000071 007 OF 008

At this time, Portugal uses facial recognition and fingerprint identification in Senegal only.

-- Does the host government issue a machine-readable passport containing biometric information? If e-Passports are issued, what biometric information is included on the document, i.e. fingerprint, iris, facial recognition, etc? If not, does host government plan to issue a biometric document in the future?

Yes, Portugal issues a machine-readable passport with biometric information. E-passports have been issued since 2006 with facial recognition technology.

1K. Identifying Appropriate Partners:

-- Department would appreciate post's assessment of whether host government would be an appropriate partner in data sharing. Considerations include whether host government watchlists may include political dissidents (as opposed or in addition to terrorists), and whether host governments would share or use U.S. watchlist data inappropriately, etc. Post recommends sharing information with Portugal. Portugal has professional, capable, and well-trained law enforcement officials who would use the information to locate and detain terrorist suspects. We have no reason to believe that Portugal would include political dissidents in any listing or use the list inappropriately.

-- Are there political realities which would preclude a country from entering into a formal data-sharing agreement with the U.S?

No, none.

-- Is the host country's legal system sufficiently developed to adequately provide safeguards for the protection and nondisclosure of information?

Yes, the legal system is well developed and able to handle the information, as outlined above.

-- How much information sharing does the host country do internally? Is there a single consolidated database, for example? If not, do different ministries share information amongst themselves?

Ministries and law enforcement agencies do share information with each other upon official request, or in accordance with the laws governing that criminal offense. Law enforcement is particularly willing to share information about major crimes, terrorism, and narcotics suspects. There is no single information sharing hub. Different agencies have access to information that relates to their area.

-- How does the country define terrorism? Are there legal statutes that do so?

In broad terms, Portuguese Law 52/2003 defines terrorism as, "All the acts that aim to facilitate, either directly or indirectly, any act committed for terrorism purposes." In

this context, it penalizes terrorist acts themselves and any instrumental offenses, such as theft or document forgery, connected with a terrorist act. Before 2003, the Penal Code had a couple of provisions with respect to terrorism and terrorist association crimes. Those provisions were partly revoked by Law 52/2003 (Law on Combating Terrorism) which transposed European Union Framework Decision 75/JAI/2002 into the Portuguese legal system.

The added value of this new Law is making individuals liable and criminalizing so-called "instrumental crimes" such as theft or document forgery, regardless of where it occurs. It also punishes the activities of groups, terrorist organizations and terrorist associations and criminalizes terrorist acts perpetrated in country as well as abroad. Additionally, the law contains some exceptions to the principle of territoriality, established in the Penal Code. Portuguese penal law may therefore be applied to acts that occur outside Portuguese territory, unless otherwise stated in an international treaty or convention, when the crimes constitute terrorist offenses committed by individuals, domestic or international organizations, provided that the agents are found on Portuguese territory and cannot be extradited to the requesting state.

Another important aspect of the law is that it envisages the criminal liability of legal persons or their equivalent (corporate and mere de facto associations) for offenses connected to terrorism when carried out on their behalf and in the interest of their organs or representatives.

LISBON 00000071 008 OF 008

Apart from Law 52/2003, there are several other laws aiming at combating terrorism:

Law 5/2002) Special regime of proof collecting and breach of professional silence regarding serious crimes;

Law 101/2001) Infiltrated agents -Juridical regime of undercover actions regarding prevention and criminal investigation;

Law 104/2001) Interception of communications; controlled deliveries; undercover actions;

Law 144/99 of 31 August (Law of International Judicial Cooperation in Criminal Matters) applies to cooperation in criminal matters. It governs extradition, transfer of proceedings in criminal matters, enforcement of criminal judgments, transfer of persons sentenced to any punishment or imprisonment, supervision of conditionally sentenced or conditionally released persons, and mutual legal assistance in criminal matters.

Law 65/2003 regarding the European Arrest Warrant regime. The European Arrest Warrant is an important cooperation tool between European Union countries and it is applicable in terrorism cases.

Law 10/2002) Monitoring mechanisms of money laundering and financing of terrorism.

Law 11/2004) Prevention and repression of money laundering law, which establishes penalties for the laundering of assets from an illicit source. This law also establishes control mechanisms to prevent crimes and terrorism.

International Instruments: In addition to the legislation cited above, Article 8 of the Portuguese Constitution states that the rules and principles of general international law are an integral part of Portuguese law. Rules provided for in international conventions that have been duly ratified or approved, shall apply in national law, following their official publication, so long as they remain internationally

binding with respect to the Portuguese state. Portugal is therefore bound to the international legal instruments, which serve as a reference to the international community in its combat against terrorism. The following are several of the multilateral and international agreements that Portugal has signed and ratified:

- UN Convention against Transnational Organized Crime (2003)
- International Convention for the Suppression of the Financing of Terrorism (2002)
- International Convention for the Suppression of Terrorist Bombings (2001)
- Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (1993)
- International Convention against Taking of Hostages (1983)
- Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (1973)

Portugal also signed, but not yet ratified, the following:

- Protocol against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition, supplementing the United Nations Convention against Transnational Organized Crime (2001) signed in 2002
 - International Convention for the Suppression of Acts of Nuclear Terrorism (2005). Signed in 2005.
- STEPHENSON